CUNOAȘTEREA ȘTIINȚIFICĂ

ISSN 2821 – 8086, ISSN – L 2821 – 8086, Volumul 3, Numărul 1, Martie 2024

Apărarea împotriva atacurilor cibernetice avansate

Nicolae SFETCU

Sfetcu, Nicolae (2024), Apărarea împotriva atacurilor cibernetice avansate, *Cunoașterea Științifică*, **3**:1, 3-16, DOI: 10.58679/CS80583, https://www.cunoasterea.ro/apararea-impotriva-atacurilor-cibernetice-avansate/

Publicat online: 06.02.2024

© 2024 Nicolae SFETCU. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Apărarea împotriva atacurilor cibernetice avansate

Ing. fiz. Nicolae SFETCU[1], MPhil
nicolae@sfetcu.com

Defense Against Advanced Cyber Attacks

Abstract

In today's digitally interconnected world, the threat of cyber attacks has become a critical concern for individuals, businesses and governments alike. Cyber attacks pose a significant risk to data privacy, financial stability, national security and even personal safety. As the sophistication and frequency of cyber threats continue to increase, it is imperative that we deploy robust defenses to protect our digital assets and infrastructure. Traditional security technology and methods are ineffective in detecting or mitigating cyber attacks. This essay explores various strategies and measures to defend against cyber attacks.
Keywords: cyber attacks, advanced persistent threat, malware, exploit, attack detection, defense, protection

Rezumat

În lumea de astăzi interconectată digital, amenințarea atacurilor cibernetice a devenit o preocupare esențială pentru indivizi, companii și guverne deopotrivă. Atacurile cibernetice reprezintă un risc semnificativ pentru confidențialitatea datelor, stabilitatea financiară, securitatea națională și chiar siguranța personală. Pe măsură ce sofisticarea și frecvența amenințărilor cibernetice continuă să crească, este imperativ să implementăm sisteme de apărare robuste pentru a ne proteja activele și infrastructura digitale. Tehnologia și metodele tradiționale de securitate sunt ineficiente în detectarea sau atenuarea atacurilor cibernetice. Acest eseu explorează diverse strategii și măsuri de apărare împotriva atacurilor cibernetice.
Cuvinte cheie: atacuri cibernetice, amenințarea persistentă avansată, malware, exploit, detectarea atacurilor, apărare, protecție

CUNOAȘTEREA ȘTIINȚIFICĂ, Volumul 3, Numărul 1, Martie 2024, pp. 3-16
ISSN 2821 – 8086, ISSN – L 2821 – 8086, DOI: 10.58679/CS80583
URL: https://www.cunoasterea.ro/apararea-impotriva-atacurilor-cibernetice-avansate/
© 2024 Nicolae SFETCU. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

[1] Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

Acesta este un articol cu Acces Deschis (Open Access) distribuit în conformitate cu termenii licenței de atribuire Creative Commons CC BY SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0/).

Introducere

În lumea de astăzi interconectată digital, amenințarea atacurilor cibernetice a devenit o preocupare esențială pentru indivizi, companii și guverne deopotrivă. Atacurile cibernetice reprezintă un risc semnificativ pentru confidențialitatea datelor, stabilitatea financiară, securitatea națională și chiar siguranța personală. Pe măsură ce sofisticarea și frecvența amenințărilor cibernetice continuă să crească, este imperativ să implementăm sisteme de apărare robuste pentru a ne proteja activele și infrastructura digitale. Acest eseu explorează diverse strategii și măsuri de apărare împotriva atacurilor cibernetice.

Tehnologia și metodele tradiționale de securitate sunt ineficiente în detectarea sau atenuarea atacurilor cibernetice. Există zeci de milioane de variante de malware[2], ceea ce face extrem de dificilă protejarea organizațiilor de atacurile cibernetice. Traficul de rețea de comandă și control poate fi detectat cu metode sofisticate. Analizele profunde ale jurnalelor și corelarea lor sunt de o utilitate limitată. Este o provocare să separați zgomotele de traficul legitim. Apărarea cibernetică activă este mai eficientă împotriva atacurilor cibernetice. Vulnerabilitățile introduse de om (HICV) sunt una din cele mai mari probleme, constituind un vector de atac semnificativ[3].

Măsuri generale împotriva atacurilor cibernetice

Principalele măsuri care se pot lua împotriva atacurilor cibernetice sunt:

1. *Monitorizarea rețelei și detectarea anomaliilor*: Implementarea sistemelor robuste de monitorizare a rețelei și de detectare a anomaliilor poate ajuta la identificarea activității atacurilor cibernetice în fazele sale incipiente. Monitorizarea constantă a traficului de rețea

[2] (Messier 2013)
[3] (Merz 2019)

și informarea cu privire la amenințările emergente prin intermediul fluxurilor de informații despre amenințări permite organizațiilor să identifice potențialele atacuri în stadiile lor incipiente. Această abordare proactivă permite răspuns rapid și atenuare.

2. *Formarea și conștientizarea angajaților*: Educarea angajaților cu privire la riscurile atacurilor cibernetice, în special prin intermediul programelor de conștientizare a phishing-ului, poate ajuta la prevenirea atacurilor de succes. Programele de formare și conștientizare a angajaților sunt cruciale în promovarea unei culturi conștiente de securitate în cadrul organizațiilor. Actualizarea și corecția regulată a software-ului și a sistemelor poate atenua riscul ca atacurile cibernetice să exploateze vulnerabilități cunoscute.
3. *Gestionarea patch-urilor*: Prima linie de apărare împotriva atacurilor cibernetice începe cu igiena cibernetică individuală și organizațională. Atacatorii cibernetici exploatează adesea vulnerabilitățile din software-ul învechit. Menținerea unui proces eficient de gestionare a corecțiilor asigură că toate sistemele și aplicațiile sunt actualizate cu cele mai recente corecții de securitate, reducând suprafața de atac și potențialele vulnerabilități. Aceasta implică adoptarea de bune practici de securitate, cum ar fi actualizarea regulată a software-ului, utilizarea parolelor puternice și unice și atenția la e-mailurile și linkurile suspecte.
4. *Firewall și sisteme de detectare a intruziunilor*: Firewall-urile acționează ca bariere între o rețea și potențialele amenințări de pe internet. Ele filtrează traficul de intrare și de ieșire, blocând accesul neautorizat și conținutul rău intenționat. Sistemele de detectare a intruziunilor (IDS) și sistemele de prevenire a intruziunilor (IPS) completează firewall-urile prin monitorizarea traficului de rețea pentru activități suspecte și luând măsuri pentru a preveni sau atenua atacurile în timp real.
5. *Soluții antivirus și anti-malware*: Implementarea unui software robust antivirus și anti-malware ajută la detectarea și eliminarea software-ului rău intenționat, inclusiv viruși, ransomware și spyware. Actualizarea regulată a acestor instrumente asigură că pot identifica și combate în mod eficient cele mai recente amenințări.
6. *Controlul accesului și autentificarea*: Implementarea măsurilor stricte de control al accesului este crucială pentru a împiedica accesul neautorizat la sisteme și date sensibile. Autentificarea cu mai mulți factori (MFA) ar trebui utilizată pentru a adăuga un nivel suplimentar de securitate dincolo de doar parole. Controlul accesului bazat pe roluri (RBAC) atribuie permisiuni pe baza rolului unei persoane, asigurându-se că numai personalul autorizat poate accesa resurse specifice.
7. *Criptarea*: Criptarea datelor sensibile atât în tranzit, cât și în repaus este un mecanism de apărare esențial. Criptarea convertește datele într-un format care nu poate fi citit, dacă nu este decriptată cu cheile adecvate. Acest lucru face extrem de dificil pentru infractorii cibernetici să acceseze sau să fure informații sensibile.
8. *Backup-uri regulate și planuri de recuperare în caz de dezastru*: Copierea de rezervă regulată a datelor critice și un plan de recuperare în caz de dezastru bine definit sunt componente esențiale ale apărării cibernetice. În cazul unui atac de succes, organizațiile își pot restaura sistemele și datele din copii de rezervă, minimizând timpul de nefuncționare și pierderea de date.
9. *Segmentarea rețelei*: Segmentarea rețelei împarte o rețea în segmente mai mici, izolate, fiecare cu acces restricționat. Acest lucru ajută la limitarea răspândirii atacurilor cibernetice în cadrul rețelei, limitând daunele potențiale cauzate de o încălcare.

10. *Securitatea punctului final*: Utilizarea unor soluții puternice de securitate pentru punctele finale poate detecta și preveni programele malware și alte amenințări legate de atacurile cibernetice.

O metodologie a Statului Major Comun al Departamentului de Apărare al Statelor Unite[4] denumită „lanțul de distrugere" (Kill Chain) este considerată un „ghid pentru direcționarea cibernetică în cinci domenii cheie: (1) identificarea pozitivă a țintelor, (2) locația țintelor, (3) atribuirea atacului, (4) perechea capacitate/țintă și (5) evaluarea potențialelor daune colaterale. Conform lui Smart, o abordare actualizată „JP 3-60" ar trebui „să introducă conceptele de centru de greutate cibernetic al unui adversar și o zonă de operațiuni comune în spațiul cibernetic. Prezența cibernetică a unui adversar constă în computere, sisteme informaționale, hardware, persoane online și așa mai departe, care pot fi separate geografic de centrul său de greutate fizic. Odată ce planificatorii identifică centrul de greutate cibernetic (un punct critic — o sursă de putere pentru operațiunile cibernetice ale adversarului), îl pot viza".[5]

Hutchins și colab.[6] susțin că o apărare eficientă împotriva atacurilor cibernetice trebuie să pună accentul pe reziliența sistemelor prin performanță și eficacitate împotriva atacurilor cibernetice.

Bere et al.[7] afirmă că cea mai bună apărare este prin evaluarea riscurilor, implementarea politicilor și controlului, campanii de conștientizare și monitorizare și evaluare, cu accent pe campaniile de conștientizare, prin politici specifice. Aceștia abordează modelul SANS de conștientizare a securității[8]. Un alt model[9] se concentrează pe reducerea amenințării de phishing

[4] (Smart 2011)
[5] (Smart 2011, 72)
[6] (Hutchins, Cloppert, and Amin 2011)
[7] (Bere et al. 2015)
[8] (Russell 2002)
[9] (Arachchilage and Love 2014)

prin influențarea comportamentului. Promovarea conștientizării se concentrează pe influențarea pozitivă a comportamentului și reducerea amenințării la securitate[10].

Detectarea atacurilor cibernetice avansate

Programele malware sunt esențiale pentru intruziunea inițială, în special exploit-uri zero-day sau instrumente evazive personalizate. Abilitatea de a detecta programe malware avansate este importantă pentru apărarea împotriva atacurilor cibernetice. Sandboxing este o tehnică dovedită pentru analizarea comportamentului malware avansat necunoscut[11]. Trebuie să se țină cont și de faptul că malware avansate pot apela la tehnici de evaziune a sandbox-ului[12].

Ghafir și Prenosil[13] au propus adăugarea de funcții la un sistem de detectare a intruziunilor open source, care să includă analiza traficului de date pe baza cererilor trimise și a protocoalelor utilizate, filtrarea folosind liste negre și utilizarea algoritmului hash în protejarea confidențialității și integrității datelor.

Wang și colab.[14] au propus o abordare bazată pe gene în detectarea amenințărilor persistente avansate folosind tiparul de atacuri preexistente.

Conform lui Adelaiye, Ajibola, și Silas[15], 72% dintre cercetători au combinat mai multe metode pentru atenuarea amenințării, considerând că metodele tradiționale sunt ineficiente. Dintre metodele adoptate, analiza traficului/datelor este cea mai utilizată, urmată de detectarea anomaliilor, recunoașterea modelelor și securitatea multistrat. Ideal ar fi să se combine cel puțin două metode. Ca a doua metodă, cea mai utilizată a fost analiza traficului/datelor urmată de recunoașterea modelelor.

[10] (Russell 2002)
[11] (Rafique et al. 2014)
[12] (Singh and Bu 2014)
[13] (Ghafir and Prenosil 2016)
[14] (Wang et al. 2014)
[15] (Adelaiye, Ajibola, and Silas 2019)

Rot și Olszewski[16] consideră că cea mai de succes formă de apărare împotriva atacurilor cibernetice este monitorizarea constantă și reacția la cât mai multe atacuri cibernetice. În 76% din cazuri, software-ul antivirus nu a reprezentat un obstacol în calea atacurilor cibernetice [17], deci protecția tradițională nu este suficientă. Practic „orice abordare eficientă de apărare împotriva atacurilor cibernetice trebuie să includă apărare în profunzime, o capacitate de detectare, un plan de răspuns la incidentele atacurilor cibernetice, un plan de recuperare și conștientizare și instruire în materie de securitate”[18]. Fiecare etapă a atacurilor cibernetice este bine cunoscută și ușor de contracarat. Problemele apar la combinația lor, cu personalizarea pentru o anumită țintă.

Apărarea bazată pe informații este o strategie care valorifică cunoștințele despre adversari și adaptează apărarea pe baza informațiilor adunate[19]. Apărătorii pot crea o buclă de feedback de informații pentru a identifica modelele încercărilor anterioare de intruziune, încercând să înțeleagă tehnicile adversarilor și apoi să pună în aplicare contramăsuri specifice.

Atenuarea atacurilor cibernetice avansate

Adelaiye, Ajibola, și Silas[20] evidențiază mai multe tehnici de atenuare a atacurilor cibernetice prin reducerea efectului advers al evenimentelor nedorite:

1. *Detectarea anomaliilor*: utilizarea unui model de comportament normal pentru comparare cu comportamentul real[21]. Detectarea anomaliilor include detectarea traficului de rețea și a activităților suspecte sau a grupurilor „neregulate” de activități (potențial obținute prin învățarea automată). Mai mulți cercetători propun utilizarea analiticei de date mari pentru detectarea atacurilor cibernetice [22].
2. *Liste albe*: atunci când accesul este permis doar la puține entități de încredere au acces[23].

[16] (Rot and Olszewski 2017)
[17] (Deloitte 2016)
[18] (Ashford 2011)
[19] (Hutchins, Cloppert, and Amin 2011)
[20] (Adelaiye, Ajibola, and Silas 2019)
[21] (Mahadevan et al. 2010)
[22] (Giura and Wang 2012)
[23] (Huh et al. 2011)

3. *Liste negre*: o listă de aplicații și procese rău intenționate cunoscute (poate preveni doar tipurile de atac pre-cunoscute)[24].
4. *Sisteme de detectare a intruziunilor (IDS)*: se bazează pe analiza porturilor, protocoalelor, adreselor IP, evenimentelor de sistem, apelurilor de sistem etc., generându-se alerte[25].
5. *Conștientizare*: atacatorii exploatează factorul uman din lanțul de securitate[26], evaluându-se, în același timp, nivelul de cunoștințe și înțelegere securității[27]. Potrivit unui studiu de conștientizarea atacurilor cibernetice [28], mai mult de jumătate dintre industrii nu sunt conștiente de diferențele dintre atacurilor cibernetice și amenințările tradiționale, iar 67% dintre respondenți raportează lipsa de formare de conștientizare în raport cu atacurile cibernetice.
6. *Înșelăciune*: prin dispozitive care ascund adevărata identitate, atacatorul este făcut să creadă că a reușit acordându-i-se acces la un sistem fals pentru a-l ține ocupat până când este identificat[29].
7. *Criptografie*: schimbând informațiile într-un format care nu poate fi înțeles[30].
8. *Trafic/Analiza datelor*: utilizarea metodelor statistice pentru analiză[31].
9. *SIEM*: instrumentul de gestionare a informațiilor de securitate și a evenimentelor (SIEM) colectează date pentru analiza potențialelor atacuri[32]. Se poate implementa o soluție de prevenire a pierderii datelor ca ultima linie de apărare[33].
10. *Recunoașterea modelelor*: detecția prin recunoașterea pe baza modului de operare[34].
11. *Evaluarea riscurilor*: prin monitorizarea activităților aplicațiilor și agregarea impactului și riscului[35].
12. *Securitate* pe mai multe straturi: comunicarea pe diferite straturi cu diverse utilizări, combinând mai multe metode din cele de mai sus implementate în planul rețelei, planul aplicației, planul utilizatorului, planul fizic etc.[36]

Metode de apărare împotriva atacurilor cibernetice avansate

Diferite metode de apărare avansate care pot fi folosite împotriva atacurilor cibernetice [37]:

1. **Metode de monitorizare:**
    1. *Monitorizarea discurilor*: prin antivirus, firewall sau filtrare de conținut, și monitorizarea CPU pentru fiecare dintre aceste sisteme.

[24] (Edwards et al. 2012)
[25] (García-Teodoro et al. 2009)
[26] (Pfleeger, Sasse, and Furnham 2014)
[27] (Bulgurcu, Cavusoglu, and Benbasat 2010)
[28] (ISACA 2016)
[29] (Nance and Bishop 2017)
[30] (Peikert 2016)
[31] (Conti et al. 2015)
[32] (Coppolino et al. 2012)
[33] (Schmid, Hill, and Ghosh 2002)
[34] (Wright et al. 2010)
[35] (Lo and Chen 2012)
[36] (Moon et al. 2014)
[37] (Alshamrani et al. 2019)

    2. *Monitorizarea memoriei*: pentru detectarea malware care poate rula în memoria sistemului mai degrabă decât dintr-un fișier, evitând urmele[38]. Duqu 2.0, care a infestat laboratoarele Kaspersky în 2015[39], a rulat în acest fel.
    3. *Monitorizarea pachetelor*: comunicarea cu Centrul de comandă și control când sistemul este compromis și pentru transferul de date ajută la identificarea comportamentelor suspecte[40].
    4. *Monitorizarea codului*: erori de cod sunt vulnerabilități prin care atacatorii pot pătrunde în sisteme. Acestea pot fi identificate prin tehnici de analiză statică, cum ar fi analiza Taint și analiza fluxului de date.
    5. *Monitorizarea jurnalelor*: poate ajuta la detectarea sau prevenirea atacurilor în stadiile incipiente, corelând jurnalele[41].
2. **Metode de detectare**
    1. *Detectarea anomaliilor*: tehnici de detectare a anomaliilor pentru a detecta diferite etape ale atacurilor cibernetice.
        1. Abordări și metode[42]
        2. Aplicare în detectarea atacurilor cibernetice [43]: tehnici AI/ML corelate cu diferite etape atacurilor cibernetice care pot fi detectate folosind tehnici AI/ML:
            1. Spear phishing
            2. Domenii DNS rău intenționate
            3. Profilarea utilizatorului
            4. Monitorizarea datelor în mișcare:
            5. Comportament anormal:
    2. Potrivirea modelelor: folosește sistemele regulate de detectare și prevenire a intruziunilor[44].
3. **Metode de atenuare**
    1. *Metode reactive*: identifică posibile scenarii de atac pe baza vulnerabilităților prezente
        1. Analiza grafică[45]
    2. *Metode proactive*: tehnici care pot înșela atacatorul sau pot modifica suprafața de atac
        1. Strategiile Honeypot și Honeynet[46]
        2. Apărarea țintei în mișcare[47].

[38] (Virvilis and Gritzalis 2013)
[39] (Kaspersky 2015)
[40] (Marchetti et al. 2016)
[41] (Shalaginov, Franke, and Huang 2016)
[42] (Hodge and Austin 2004)
[43] (Kim et al. 2015)
[44] (Yan and Zhang 2013)
[45] (Johnson and Hogan 2013)
[46] (Bowen et al. 2009)
[47] (Crouse, Prosser, and Fulp 2015)

Protecția stratificată

Principalele tipuri de apărare împotriva atacurilor cibernetice se bazează pe hardware și pe cloud[48]. Soluțiile bazate pe hardware implică un dispozitiv dedicat care monitorizează traficul suspect pe baza indicilor de reputație și face analize comportamentale și sandboxing. Acestea au unele limite, nu sunt capabile să înregistreze întregul trafic de rețea. Soluțiile bazate pe cloud, furnizate ca o platformă multi-utilizator, ar trebui să evite aceste limitări și să monitorizare mai eficient traficul, realizând o analiză holistică (comportament, vulnerabilități, filtrarea adreselor, monitorizarea transmisiei SSL, conținut activ etc.). Cele mai eficiente sunt modelele de protecție stratificată[49]:

1. *Model de protecție împotriva atacurilor cibernetice cu mai multe straturi*: se bazează pe apărarea în profunzime, care implică protecția atentă a fiecărui strat al rețelei: oamenii, dispozitivele și aplicațiile[50].
2. *Platforma SIEM ca formă de apărare împotriva atacurilor*: implementarea instrumentelor SIEM (Security Information and Event Management) de a doua generație pentru gestionarea informațiilor referitoare la securitate și incidente. SIEM oferă „colectare și arhivare a datelor, analiză detaliată a evenimentelor și normalizării, rapoarte, interogări și, de obicei, o formă de modul de analiză în timp real”[51].
3. *Tehnologia big data în detectarea și rezistența la atacurile cibernetice*: numită și SIEM de a doua generație, printr-o analiză integrată a jurnalului și detectarea anomaliilor bazate pe un model tipic personalizat pentru o anumită organizație[52] sau analiză comportamentală. Soluțiile bazate pe MapReduce, Hadoop sau Hive permit scurtarea timpului de analiză de aproximativ douăzeci de ori[53].

Apărarea împotriva unui atac cibernetic nu poate fi făcută cu un singur instrument[54]. Corelarea evenimentelor joacă un rol cheie în protejarea în profunzime, prin adoptarea mai multor nivele de apărare. L. Yang şi colab.[55] au modelat definind echilibrul rețelei cibernetice ca măsură

[48] (Rot 2016)
[49] (Rot and Olszewski 2017)
[50] (Hudson 2013)
[51] (Muszyński and Shipley 2008)
[52] (Kim et al. 2015)
[53] (Zions Bancorporation 2012)
[54] (Alshamrani et al. 2019)
[55] (Yang et al. 2017)

de securitate au studiat și au analizat teoretic alți factori asupra acestui echilibru și au raportat că securitatea de echilibru a unei rețele cibernetice va scădea odată cu adăugarea de noi margini la rețea. Securitatea de echilibru atinge maxim atunci când resursele de prevenire sunt apropiate de cea de resurse de recuperare și că aceeași valoare crește odată cu creșterea resurselor de apărare pe unitatea de timp. Ei recomandă distribuirea resurselor de apărare în mod egal între prevenire și recuperare, și sugerează că configurarea mai multor resurse este eficientă în protecția împotriva atacurilor cibernetice.

Sisteme de apărare împotriva atacurilor cibernetice avansate

Planurile de răspuns la incidente bine documentate și politici de securitate cibernetică, asigură că organizațiile pot răspunde eficient atunci când are loc un atac cibernetic. Procedurile clare pentru raportarea, limitarea și recuperarea în urma incidentelor sunt esențiale pentru a minimiza daunele și pentru a reduce timpul de nefuncționare. Datorită caracteristicilor specifice ale atacurilor cibernetice, nu există o soluție unică de protecție eficientă. Cea mai bună practică actuală este o gamă largă de contramăsuri de securitate care au ca rezultat o apărare pe mai multe straturi. Unele dintre sistemele de apărare existente trebuie reproiectate pentru a funcționa în contextul atacurilor cibernetice.

Nume	**Operațiunea Aurora**[56]	**Atacul RAS**[57]	**Operațiunea Ke3chang**[58]	**Operațiunea SnowMan**[59]
Timp activ	iunie 2009 - decembrie 2009	Necunoscut - martie 2011	mai 2010 - decembrie 2013	Necunoscut - februarie 2014
Recunoaștere și înarmare	e-mailurile angajaților, exploatările zero-day,	e-mailurile angajaților, exploit-uri zero-day,	e-mailurile oficialilor, documente troianizare,	identificați punctele slabe în vfw.org, RAT, backdoor

[56] (McAfee 2010)
[57] (Greenberg, n.d.)
[58] (Villeneuve et al. 2013)
[59] (Leonhard 2014)

	backdoor și instrumentele C&C	documente troianizate, backdoor, RAT	backdoor și instrumente C&C	
Livrare	spear phishing (linkuri rău intenționate)	spear phishing (fișier xls rău intenționat)	spear phishing (fișier zip rău intenționat)	atacul la gura de apă (compromite și infectează)
Intruziunea inițială	descărcare drive-by (CVE-2010-0249)	vulnerabilitatea xls (CVE-2011-0609)	victimele deschid fișierul executabil	descărcare drive-by (CVE-2014-0322)
Comandă și control	protocol C2 personalizat, care funcționează pe portul TCP 443	Poison Ivy RAT	protocol C2 personalizat, bazat pe protocolul HTTP	ZxShell, Gh0st RAT
Mișcare laterală	compromite SCM și obține codul sursă	efectuează escaladarea privilegiilor, adună date SecureID	compromite sistemele interne, colectează date	necunoscut
Exfiltrarea datelor	încarcă date pe serverele C&C	comprimă, criptează datele ca fișiere RAR, utilizează FTP pentru transmitere	comprimă, criptează datele ca fișiere RAR	necunoscut, ar putea fi informații militare americane

Tabelul 2: Comparația diferitelor atacuri cibernetice. Sursa[60]. Traducere și adaptare: Nicolae Sfetcu

Tehnici de atac și contramăsuri în fiecare etapă a unui atac cibernetic:

Etape	Tehnici/instrumente de atac	Contramăsuri
Recunoaștere și înarmare	OSINT, inginerie socială, pregătirea programelor malware	Instruire de conștientizare a securității, gestionarea corecțiilor, firewall
Livrare	Spear phishing, atac în gura de apă	Software de filtrare a conținutului, NIDS, software antivirus
Intruziunea inițială	Exploatări zero-day, execuție de cod de la distanță	Gestionarea corecțiilor, HIDS, detectare avansată a malware
Comanda și control	Exploatarea serviciilor legitime, RAT, criptare	NIDS, SIEM, detectarea anomaliilor de eveniment
Mișcarea laterală	Escaladarea privilegiilor, colectarea datelor	Controlul accesului, HIDS, NIDS, detectarea anomaliilor evenimentelor
Exfiltrarea datelor	Compresie, criptare, etapă intermediară	Prevenirea pierderilor de date

Tabelul 3: Tehnici de atac și contramăsuri în fiecare etapă a unui atac cibernetic. Sursa[61]. Traducere și adaptare: Nicolae Sfetcu

Concluzie

Atacurile cibernetice sunt o amenințare mereu prezentă și în evoluție în era noastră digitală. Indivizilor, întreprinderilor și guvernelor le revine obligația de a lua măsuri proactive pentru a se

[60] (Chen, Desmet, and Huygens 2014)
[61] (Chen, Desmet, and Huygens 2014)

apăra împotriva acestor amenințări. Implementarea unei abordări pe mai multe straturi care combină cele mai bune practici de securitate cibernetică, soluții tehnologice avansate și monitorizare vigilentă este esențială pentru atenuarea riscurilor asociate atacurilor cibernetice. Numai prin prioritizarea și investiții în strategii robuste de apărare cibernetică putem spera să ne protejăm activele digitale și să menținem integritatea și securitatea lumii noastre interconectate.

Bibliografie

Adelaiye, Oluwasegun, Aminat Ajibola, and Faki Silas. 2019. "Evaluating Advanced Persistent Threats Mitigation Effects: A Review," February.

Alshamrani, Adel, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. 2019. "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities." *IEEE Communications Surveys & Tutorials* 21 (2): 1851–77. https://doi.org/10.1109/COMST.2019.2891891.

Arachchilage, Nalin, and Steve Love. 2014. "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective." *Computers in Human Behavior* 38 (September): 304–12. https://doi.org/10.1016/j.chb.2014.05.046.

Ashford, Warwick. 2011. "How to Combat Advanced Persistent Threats: APT Strategies to Protect Your Organisation | Computer Weekly." ComputerWeekly.Com. 2011. https://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation.

Bere, Mercy, Fungai Bhunu Shava, Attlee Gamundani, and Isaac Nhamu. 2015. "How Advanced Persistent Threats Exploit Humans." *IJCSI*, November.

Bowen, Brian M., Shlomo Hershkop, Angelos D. Keromytis, and Salvatore J. Stolfo. 2009. "Baiting Inside Attackers Using Decoy Documents." In *Security and Privacy in Communication Networks*, edited by Yan Chen, Tassos D. Dimitriou, and Jianying Zhou, 51–70. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-05284-2_4.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–48. https://doi.org/10.2307/25750690.

Chen, Ping, Lieven Desmet, and Christophe Huygens. 2014. "A Study on Advanced Persistent Threats." In *Communications and Multimedia Security*, edited by Bart De Decker and André Zúquete, 63–72. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-44885-4_5.

Conti, Mauro, Luigi V. Mancini, Riccardo Spolaor, and Nino Vincenzo Verde. 2015. "Can't You Hear Me Knocking: Identification of User Actions on Android Apps via Traffic Analysis." In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 297–304. CODASPY '15. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2699026.2699119.

Coppolino, L., Michael Jäger, Nicolai Kuntze, and Roland Rieke. 2012. “A Trusted Information Agent for Security Information and Event Management.” In , 6–12.

Crouse, Michael, Bryan Prosser, and Errin Fulp. 2015. *Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses*. https://doi.org/10.1145/2808475.2808480.

Deloitte. 2016. “Cyber Espionage - The Harsh Reality of Advanced Security Threats.” https://indianstrategicknowledgeonline.com/web/us_aers_cyber_espionage_07292011.pdf.

Edwards, Benjamin, Tyler Moore, George Stelle, Steven Hofmeyr, and Stephanie Forrest. 2012. “Beyond the Blacklist: Modeling Malware Spread and the Effect of Interventions.” *Proceedings New Security Paradigms Workshop*, February. https://doi.org/10.1145/2413296.2413302.

García-Teodoro, Pedro, Jesús Díaz-Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez. 2009. “Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges.” *Computers & Security* 28 (February): 18–28. https://doi.org/10.1016/j.cose.2008.08.003.

Ghafir, Ibrahim, and Vaclav Prenosil. 2016. “Proposed Approach for Targeted Attacks Detection.” In *Advanced Computer and Communication Engineering Technology*, edited by Hamzah Asyrani Sulaiman, Mohd Azlishah Othman, Mohd Fairuz Iskandar Othman, Yahaya Abd Rahim, and Naim Che Pee, 73–80. Lecture Notes in Electrical Engineering. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-24584-3_7.

Giura, P., and Wei Wang. 2012. “Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats.” *Science*. https://www.semanticscholar.org/paper/Using-Large-Scale-Distributed-Computing-to-Unveil-Giura-Wang/75e702d56a4a90f9c773a0e1fd0074cbe6910ead.

Greenberg, Andy. n.d. “The Full Story of the Stunning RSA Hack Can Finally Be Told.” *Wired*. Accessed December 11, 2023. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/.

Hodge, Victoria J., and Jim Austin. 2004. “A Survey of Outlier Detection Methodologies.” *Artificial Intelligence Review* 22 (2): 85–126. https://doi.org/10.1007/s10462-004-4304-y.

Hudson, Barbara. 2013. “Advanced Persistent Threats: Detection, Protection and Prevention.” https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Sophos_Advanced_Persistent_Threats.pdf.

Huh, Jun, John Lyle, Cornelius Namiluko, and Andrew Martin. 2011. “Managing Application Whitelists in Trusted Distributed Systems.” *Future Generation Comp. Syst.* 27 (February): 211–26. https://doi.org/10.1016/j.future.2010.08.014.

Hutchins, Eric, Michael Cloppert, and Rohan Amin. 2011. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” *Leading Issues in Information Warfare & Security Research* 1 (January).

ISACA. 2016. “Book Review: Advanced Persistent Threats.” ISACA. 2016. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/advanced-persistent-threats-how-to-manage-the-risk-to-your-business.

Johnson, John, and Emilie Hogan. 2013. *A Graph Analytic Metric for Mitigating Advanced Persistent Threat*. Vol. 129. https://doi.org/10.1109/ISI.2013.6578801.

Kaspersky. 2015. “The Duqu 2.0.” https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf.

Kim, Hyunjoo, Jonghyun Kim, Ikkyun Kim, and Tai-myung Chung. 2015. “Behavior-Based Anomaly Detection on Big Data.” *Australian Information Security Management Conference*, January. https://doi.org/10.4225/75/57b69d1ed938e.

Leonhard, Woody. 2014. “Internet Explorer ‘SnowMan’ Zero-Day Spreading: Use Alternative or Patch with KB 2934088.” InfoWorld. February 26, 2014. https://www.infoworld.com/article/2610582/internet-explorer--snowman--zero-day-spreading--use-alternative-or-patch-with-kb-293408.html.

Lo, Chi-Chun, and Wan-Jia Chen. 2012. “A Hybrid Information Security Risk Assessment Procedure Considering Interdependences between Controls.” *Expert Systems with Applications* 39 (1): 247–57. https://doi.org/10.1016/j.eswa.2011.07.015.

Mahadevan, Vijay, Wei-Xin LI, Viral Bhalodia, and Nuno Vasconcelos. 2010. *Anomaly Detection in Crowded Scenes*. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. https://doi.org/10.1109/CVPR.2010.5539872.

Marchetti, Mirco, Fabio Pierazzi, Michele Colajanni, and Alessandro Guido. 2016. “Analysis of High Volumes of Network Traffic for Advanced Persistent Threat Detection.” *Computer Networks* 109 (June). https://doi.org/10.1016/j.comnet.2016.05.018.

McAfee. 2010. “Protecting Your Critical Assets - Lessons Learned from ‘Operation Aurora.’” https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

Merz, Terry. 2019. “A Context-Centred Research Approach to Phishing and Operational Technology in Industrial Control Systems | Journal of Information Warfare.” 2019. https://www.jinfowar.com/journal/volume-18-issue-4/context-centred-research-approach-phishing-operational-technology-industrial-control-systems.

Messier, Ric. 2013. *GSEC GIAC Security Essentials Certification All-in-One Exam Guide*. McGraw Hill Professional.

Moon, Daesung, Hyungjin Im, Jae Dong Lee, and Jong Hyuk Park. 2014. “MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats.” *Symmetry* 6 (4): 997–1010. https://doi.org/10.3390/sym6040997.

Muszyński, Józef, and Greg Shipley. 2008. “Narzędzia SIEM (Security Information and Event Management).” Computerworld. 2008. https://www.computerworld.pl/news/Narzedzia-SIEM-Security-Information-and-Event-Management,325855.html.

Nance, Kara, and Matt Bishop. 2017. *Introduction to Deception, Digital Forensics, and Malware Minitrack*. https://doi.org/10.24251/HICSS.2017.731.

Peikert, Chris. 2016. “A Decade of Lattice Cryptography.” *Foundations and Trends® in Theoretical Computer Science* 10 (4): 283–424. https://doi.org/10.1561/0400000074.

Pfleeger, Shari, Angela Sasse, and Adrian Furnham. 2014. “From Weakest Link to Security Hero: Transforming Staff Security Behavior.” *Journal of Homeland Security and Emergency Management* 11 (December). https://doi.org/10.1515/jhsem-2014-0035.

Rafique, M. Zubair, Ping Chen, Christophe Huygens, and Wouter Joosen. 2014. “Evolutionary Algorithms for Classification of Malware Families through Different Network Behaviors.” In *Proceedings of the 2014 Annual Conference on Genetic and Evolutionary Computation*, 1167–74. GECCO ’14. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2576768.2598238.

Rot, Artur. 2016. “Zarządzanie Ryzykiem w Cyberprzestrzeni – Wybrane Zagadnienia Teorii i Praktyki.” In , 35–50.

Rot, Artur, and Bogusław Olszewski. 2017. *Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection*. https://doi.org/10.15439/2017F488.

Russell, Chelsa. 2002. “Security Awareness - Implementing an Effective Strategy | SANS Institute.” 2002. https://www.sans.org/white-papers/418/.

Schmid, M., F. Hill, and A.K. Ghosh. 2002. “Protecting Data from Malicious Software.” *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 199–208. https://doi.org/10.1109/CSAC.2002.1176291.

Shalaginov, Andrii, Katrin Franke, and Xiongwei Huang. 2016. *Malware Beaconing Detection by Mining Large-Scale DNS Logs for Targeted Attack Identification*.

Singh, Abhishek, and Zheng Bu. 2014. “Hot Knives Through Butter: Bypassing Automated Analysis Systems (Black Hat USA 2013) - InfoconDB.” 2014. https://infocondb.org/con/black-hat/black-hat-usa-2013/hot-knives-through-butter-bypassing-automated-analysis-systems.

Smart, Steven J. 2011. “Joint Targeting in Cyberspace.” https://apps.dtic.mil/sti/citations/ADA555785.

Villeneuve, Nart, James T. Bennett, Ned Moran, Thoufique Haq, Mike Scott, and Kenneth Geers. 2013. *Operation "Ke3chang: Targeted Attacks Against Ministries of Foreign Affairs*. FireEye, Incorporated.

Virvilis, Nikos, and Dimitris Gritzalis. 2013. “The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?” In *2013 International Conference on Availability, Reliability and Security*, 248–54. https://doi.org/10.1109/ARES.2013.32.

Wang, Yuan, Yongjun Wang, Jing Liu, and Zhijian Huang. 2014. “A Network Gene-Based Framework for Detecting Advanced Persistent Threats.” In *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 97–102. https://doi.org/10.1109/3PGCIC.2014.41.

Wright, John, Yi Ma, Julien Mairal, Guillermo Sapiro, Thomas S. Huang, and Shuicheng Yan. 2010. “Sparse Representation for Computer Vision and Pattern Recognition.” *Proceedings of the IEEE* 98 (6): 1031–44. https://doi.org/10.1109/JPROC.2010.2044470.

Yan, Xiaohuan, and J. Zhang. 2013. “A Early Detection of Cyber Security Threats Using Structured Behavior Modeling.” In . https://www.semanticscholar.org/paper/A-Early-Detection-of-Cyber-Security-Threats-using-Yan-Zhang/92b0c21afbf1941cb27e707c50e51bd76a8b1d45.

Yang, Lu Xing, Pengdeng Li, Xiaofan Yang, and Yuan Yan Tang. 2017. “Security Evaluation of the Cyber Networks under Advanced Persistent Threats.” *IEEE Access* 5 (8053761): 20111–23. https://doi.org/10.1109/ACCESS.2017.2757944.

Zions Bancorporation. 2012. “A Case Study In Security Big Data Analysis.” 2012. https://www.darkreading.com/cybersecurity-analytics/a-case-study-in-security-big-data-analysis.